(19) **RU** (11) **2 126 168** (13) **C1**

(51) МПК[6] **G 06 F 12/14**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 97104793/09, 02.04.1997

(46) Дата публикации: 10.02.1999

(56) Ссылки: RU 94 020 949 A1, 27.02.96. EP 0 3750900 A1, 04.07.90. RU 95 100 344 A1, 10.11.96. EP 0 614 147 A2, 07.09.94.

(98) Адрес для переписки:
121165 Москва, а/я 115, ООО "Юстис" патентному поверенному Груниной А.Е.

(71) Заявитель:
Варшавский Зиновий Матвеевич,
Красовский Сергей Яковлевич,
Рубанов Владимир Осипович,
Стребков Анатолий Иванович

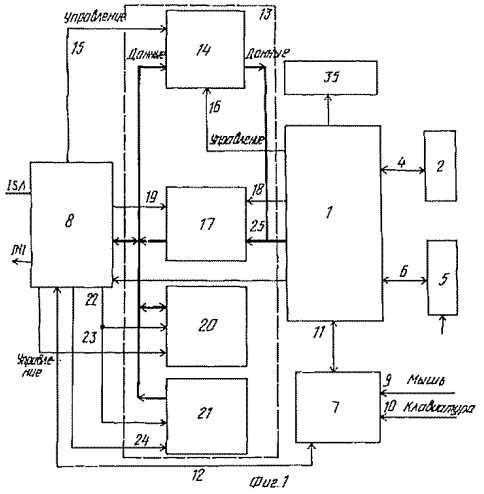
(72) Изобретатель: Варшавский З.М.,
Красовский С.Я., Рубанов В.О., Стребков А.И.

(73) Патентообладатель:
Товарищество с ограниченной ответственностью "Коминфор" ("Cominfor")

(54) СПОСОБ ЗАЩИТЫ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА И УСТРОЙСТВО ДЛЯ ЕГО РЕАЛИЗАЦИИ

(57) Реферат:

Изобретение относится к области вычислительной техники. Технический результат достигается повышением функциональной надежности защиты путем упрощения способа и создания надежного и простого в эксплуатации устройства защиты от несанкционированного доступа, подключенного к системной шине персонального компьютера, как ключа для разрешения доступа к ПК, без физического соединения с которым компьютер не сможет работать. 2 с. и 4 з.п. ф-лы, 2 ил.



Фиг.1

RU 2126168 C1

RU 2126168 C1

(19) **RU** (11) **2 126 168** (13) **C1**

(51) Int. Cl.[6] **G 06 F 12/14**

RUSSIAN AGENCY
FOR PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application 97104793/09, 02.04.1997

(46) Date of publication: 10.02.1999

(98) Mail address:
121165 Moskva, a/ja 115, OOO "Justis"
patentnomu poverennomu Gruninoj A.E.

(71) Applicant:
Varshavskij Zinovij Matveevich,
Krasovskij Sergej Jakovlevich,
Rubanov Vladimir Osipovich,
Strebkov Anatolij Ivanovich

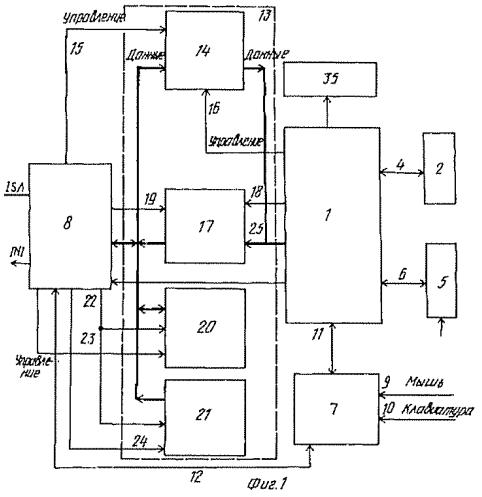
(72) Inventor: Varshavskij Z.M.,
Krasovskij S.Ja., Rubanov V.O., Strebkov A.I.

(73) Proprietor:
Tovarishchestvo s ogranichennoj
otvetstvennost'ju "Kominfor" ("Cominfor")

(54) METHOD FOR PROTECTION OF PERSONAL COMPUTER AGAINST UNAUTHORIZED ACCESS AND DEVICE WHICH IMPLEMENTS SAID METHOD

(57) Abstract

FIELD computer engineering. SUBSTANCE: device is designed as access system, which is connected to system bus of personal computer and performs physical connection without which computer does not work. EFFECT: increased reliability of protection, simplified method and device design. 6 cl, 2 dwg



Фиг.1

RU 2126168 C1

RU 2126168 C1

Способ и устройство защиты персонального компьютера от несанкционированного доступа относятся к области вычислительной техники и могут быть использованы как индивидуально самим владельцем компьютера, так и в корпоративных системах, имеющих администратора безопасной эксплуатации. Способ может быть реализован устройством, которое является функционально законченным модулем, содержащим в составе микроЭВМ. Конструктивно устройство устанавливается в персональном компьютере таким образом, чтобы подключить устройство защиты к шине компьютера.

Из уровня техники известен способ защиты персонального компьютера от несанкционированного доступа, заключающийся в том, что запоминают идентификационные коды различных режимов работы и пользователей, сравнивают идентификационные коды и по результатам сравнения реализуют различные виды доступа к вычислительной системе (см. ЕР, заявка, 0478126, кл. G 06 F 13/12, 1992).

Известна система на базе связанных между собой шиной компьютера и внешнего устройства. Система содержит микропроцессор в составе микроЭВМ, подключенное к нему с помощью последовательной шины устройство, имеющее многоразрядный адрес и содержащее регистр для хранения битов данных, имеющих многоразрядные адреса, используемые микропроцессором при доступе к регистрам. Микропроцессор содержит генератор сообщения доступа к регистру. В многоразрядном регистре первое количество разрядов содержит многоразрядный адрес внешнего устройства, второе количество разрядов предназначено для идентификации сообщения, один разряд предназначен для идентификации режима записи или считывания, третье количество разрядов предназначено для определения адреса последнего доступа регистра.

К микропроцессору подключен блок для последовательной передачи сообщений по шине во внешнее устройство. Внешнее устройство содержит блок для приема сообщения о доступе к регистру, подключенный к шине, и блок, включенный между блоком приема и регистрации для разрешения доступа к регистру в соответствии с адресом, определяемым третьим количеством разрядов второго переданного сообщения (см. там же).

В известной системе доступ к системе осуществляется путем сложной защиты частей системы программными средствами.

Наиболее близким по технической сущности к данному способу является способ защиты персонального компьютера от несанкционированного доступа, заключающийся в том, что предварительно вводят идентификационные коды системы, предназначенные для хранения, вводят идентификационный код пользователя, сравнивают идентификационный код пользователя с идентификационными кодами системы, при совпадении указанного кода по крайней мере с одним из идентификационных кодов системы осуществляют доступ к системе (RU, 95100344, G 06 F 12/14, 10.11.96).

Наиболее близким к заявленному устройству является устройство защиты компьютера от несанкционированного доступа, содержащие микроЭВМ, связанную с запоминающим устройством, блоком ввода идентификационного кода и схемой сопряжения с компьютером.

В известных способе и устройстве доступ к персональному компьютеру осуществляют следующим образом. Контрольный процессор в составе микроЭВМ осуществляет проверку идентификационного кода доступа. Процессор управления доступом в составе микроЭВМ осуществляет проверку идентификационного кода доступа, в режиме проверки процессор получает команды с центрального процессора, осуществляют проверку и формирует сообщения для обмена информацией о прерывании состояния и управлении. Поскольку в известных способе и устройстве доступ в персональный компьютер осуществляют только программно, т.е. путем анализа сообщений и формирования команд, то система в целом не обладает надежной защитой от несанкционированного доступа.

Все перечисленные известные способы для защиты от несанкционированного доступа в компьютер или к памяти и устройства, их реализующие, имеют на входе в систему специальные средства идентификации, являющиеся частью самой системы, идентифицирующей пользователя программно.

Это приводит к тому, что доступ может получить недобросовестный пользователь в отсутствие владельца, зная общий алгоритм или код входа в систему.

Данное изобретение использует представление о том, что персональный компьютер используется одним конкретным пользователем (владельцем) "персонально", а потому нет необходимости разделять его ресурсы и защищать полученные части по отдельности. Отсюда, основной задачей защиты компьютера от несанкционированного доступа является исключение возможности управления им посторонним лицом в отсутствие владельца.

Техническим результатом предложения является повышение функциональной надежности защиты путем упрощения способа и создания надежного и простого в эксплуатации устройства защиты от несанкционированного доступа, подключенного к системной шине персонального компьютера (ПК), как ключа для разрешения доступа к ПК, без физического соединения с которым компьютер не сможет функционировать.

Создание выделенного активного процессорного элемента в виде устройства защиты (микропроцессор или микроЭВМ), решающего исключительно задачи идентификации пользователей и разграничения доступа.

Хранение всех программ в ПЗУ (постоянного запоминающего устройства) устройства с целью исключения их искажений другой программой, человеком или вирусом.

В частности, в состав устройства входит сменный идентификатор кодов системы, который, в зависимости от задач компьютера, может хранить разные наборы идентификационных кодов системы.

Блокировка доступа к ПК путем

RU 2126168 C1

RU 2126168 C1

физического отключения устройств ввода (клавиатура, мышь и т.п.), выполняемого автоматически, при удалении средства или устройства для идентификации пользователя.

Минимальное использование аппаратных ресурсов ПК - только одну линию аппаратного прерывания (память, порты и диски не используются с целью не вносить каких-либо ограничений в работу ПК)

Технический результат достигается тем, что в способе защиты персонального компьютера от несанкционированного доступа, заключающемся в том, что предварительно вводят идентификационные коды системы, предназначенные для хранения, вводят идентификационный код пользователя, сравнивают идентификационный код пользователя с идентификационными кодами системы, при совпадении указанного кода по крайней мере с одним из идентификационных кодов системы реализуют доступ к системе, причем доступ к системе осуществляют путем замыкания цепи, соединяющей устройство ввода персонального компьютера с персональным компьютером.

При реализации доступа к системе при совпадении указанных кодов формируют команду управления включением указанной цепи, по которой осуществляют ее замыкание.

Технический результат достигается также тем, что в устройство защиты персонального компьютера от несанкционированнного доступа, содержащее микроЭВМ, запоминающее устройство, блок ввода идентификационного кода пользователя, схему сопряжения с персональным компьютером, введены идентификатор кодов системы, формирователь сигнала блокировки, первый и второй вход-выходы микроЭВМ соединены со входами-выходами соответственно идентификатора кодов системы и блока идентификационного кода пользователя, третий вход-выход соединен с управляющим входом формирователя сигнала блокировки, включенного в цепь устройства ввода персонального компьютера, соединенную с соответствующим входом схемы сопряжения с персональным компьютером, шина данных микроЭВМ соединена с шиной данных запоминающего устройства, управляющий выход микроЭВМ соединен с первым и вторым управляющими входами запоминающего устройства, шина схемы сопряжения с персональным компьютером соединена с соответствующими шинами запоминающего устройства, управляющие выходы, подключены к соответствующим входам запоминающего устройства.

В устройство введен звукоизлучатель, соединенный с сигнальным выходом микроЭВМ.

Формирователь сигнала блокировки выполнен в виде управляемого размыкающего ключа. Идентификатор кодов системы выполнен в виде энергонезависимого блока памяти.

На фиг. 1 представлена блок-схема предложенного устройства защиты персонального компьютера от несанкционированного доступа, реализующего предложенный способ, на фиг. 2 представлена блок-схема устройства, в котором представлен другой вариант выполнения запоминающего устройства.

Устройство содержит микроЭВМ 1, предназначенную для управления работой устройства, идентификатор 2 кодов системы, который предназначен для хранения системного журнала, перечня пользователей, допущенных к работе с ПК, а также программных кодов, обеспечивающих функционирование микроЭВМ 1. Обмен информацией между идентификатором 2 и микроЭВМ 1 осуществляется по связям 3, 4.

Блок 5 ввода идентификационного кода пользователя предназначен для хранения информации, идентифицирующей пользователя и определяющей его категорию и права доступа к компьютеру или информационной системе. Обмен информацией между блоком 5 и микроЭВМ 1 осуществляется по связи 6. В качестве блоков 2 и 5 могут использоваться устройства, имеющие в своем составе энергонезависимую память необходимого объема, например персональные идентификаторы фирмы Dallas Semiconductor.

Формирователь 7 сигнала блокировки предназначен для обеспечения связи между устройствами ввода персонального компьютера (клавиатуры ПК и манипулятора типа "мышь") и схемой сопряжения с персональным компьютером. В случае если блок 5 не установлен или пользователь не допущен к работе с данным ПК, формирователь сигнала блокировки 7 на физическом уровне отключает клавиатуру или мышь от ПК. Связи 9 и 10 предназначены для подключения мыши и клавиатуры к устройству. Связь 11 обеспечивает информационный обмен между формирователем 7 и микроЭВМ 1. Связь 12 обеспечивают информационный обмен между устройствами ввода компьютера (клавиатура, мышь) и схемой 8 сопряжения с персональным компьютером, непосредственно связанной с компьютером при нормальной работе устройства. Запоминающее устройство 13 (фиг. 1) может быть выполнено на регистре 14 приема данных из ПК с управляющим входом 15 и 16, регистре 17 передачи данных в ПК с управляющими входами 18 и 19, блоке 20 оперативной памяти и блоке 21 постоянной памяти (BIOS) с управляющими входами 22, 23 и 24, шина данных 25, шина 26.

В другом варианте выполнения запоминающее устройство 13 (фиг. 2) соединено с микроЭВМ 1 шиной 25 данных и шиной 27 управления и со схемой 8 сопряжения с ПК шиной 26 и шинами 28. В этом случае ЗУ 13 состоит из блока 29 постоянной памяти (BIOS), содержащего программы устройства при загрузке операционной системы, обработчика 30 прерываний, содержащего программы обработки прерывания, поступающих из устройства в ПК, блока 31 оперативной памяти, предназначенного для хранения оперативной информации, необходимой при выполнении программ BIOS, и обработчика 30 прерываний, регистра 32 состояний, предназначенного для передачи состояний устройства в ПК во время работы программ BIOS и обработчика прерываний, регистра данных 33, предназначенного для обмена информацией между устройством и ПК во время программ BIOS и обработчика

RU 2126168 C1

RU 2126168 C1

прерывания, регистра 34 синхронизации обмена, предназначенного для синхронизации совместной работы устройства и ПК.

Запоминающее устройство устроено так, что оно физически расположено в устройстве, а логически находится в адресном пространстве ПК. Во время работы программ BIOS и обработчика прерывания память ПК не используется. Блоки BIOS и обработчика прерывания выполнены на базе ПЗУ, а остальные - на базе ОЗУ.

Схема 8 сопряжения с ПК предназначена для объединения шин 26 и 28 (сигналы адреса, данных и синхронизации) в шину, которая непосредственно соединяется с системной шиной ПК.

Звукоизлучатель 35 предназначен для формирования звуковых сигналов в процессе работы устройства при обнаружении нарушений порядка доступа.

Устройство защиты вместе с персональным компьютером составляют систему, в которой пользователь идентифицируется по информации, хранящейся в его персональном идентификаторе (на чертеже не показан). Эти идентификаторы представляют собой малогабаритные микросхемы с собственной энергонезависимой памятью, заключенные в герметичный металлический корпус, имеющий форму таблетки. Они надежно защищены от внешних воздействий и способны хранить информацию более десяти лет. Важнейшим свойством такого идентификатора является его уникальность, который обеспечивается изготовителем путем записи в его неизменяемую память индивидуального серийного номера. Считывание этого номера позволяет надежно идентифицировать пользователя персонального компьютера. Устройство защиты персонального компьютера от несанкционированного доступа работает следующим образом.

При включении персонального компьютера управление передается процедуре инициализации устройства, расположенного в виде отдельной платы, (на чертеже не показана). Устройство приостанавливает загрузку и запрашивает пароль пользователя. Перед, тем, как ввести пароль, пользователь должен установить в специальное контактное устройство 36, подключенное ко входу блока 5 ввода идентификационного кода пользователя, свой персональный идентификатор (на чертеже не показан). Введенный пароль проверяется процессором устройства микроЭВМ 1 с помощью специальной процедуры и при положительном результате этой проверки тот же процессор проверяет факт наличия данного персонального идентификатора в перечне допущенных к работе на данном персональном компьютере. Этот перечень хранится в идентификаторе 2 кодов системы. Если этот факт установлен, то работа персонального компьютера продолжается в обычном режиме. Необходимо отметить, что все действия, связанные с идентификацией пользователя выполняются микроЭВМ 1 предложенного устройства, который недоступен центральному процессору персонального компьютера, это делает процедуру идентификации недоступной для любого вмешательства извне.

В дальнейшем, как только пользователь удалит свой персональный идентификатор из контактного устройства 36 происходит блокировка клавиатуры и мыши по каналам 9 и 10 компьютера, чем исключается возможность несанкционированнного доступа со стороны постороннего лица, хотя компьютер и продолжает функционировать. После возврата персонального идентификатора клавиатура и мышь становятся доступными, при этом в зависимости от конфигурации, хранящейся в памяти устройства, может быть вновь затребован ввод пароля. Блокировка клавиатуры и мыши производится собственным процессором устройства путем физического разрыва линий связи этих устройств с персональным компьютером.

Отличительной особенностью устройства является также то, что устройство непрерывно контролирует работу персонального компьютера и все ее действия производятся на физическом уровне и не зависят от операционной среды и режима работы ПК.

Устройство защиты выполняет все функции исключительно с помощью собственных ресурсов и не использует ни оперативную память ПК, ни его диск.

Способ и устройство для его реализации обеспечивает реализацию следующих функций парольную защиту, хранение идентифицирующей информации в надежных персональных идентификаторах типа touch memory, постоянный контроль целостности системы (неизменность вектора прерывания, условий физического подключения и т.д.) и, по возможности, ее самовосстановление, постоянное подтверждение блокировки клавиатуры и мыши при удалении идентификатора пользователя, что существенно повышает надежность блокировки, выдачу звукового сигнала с помощью установленного на плате звукоизлучателя при невозможности нейтрализации несанкционированных действий, ведение защищенного системного журнала.

Устройство защиты, размещенное на отдельной плате практически не влияет на работу компьютера в любом из возможных режимов и не изменяет его эксплуатационные характеристики.

Устройство выполняет свои функции на физическом уровне, используя лишь прерывания BIOS. В связи с этим ее работа не зависит от операционной системы, установленной на персональном компьютере.

Устройство размещено, как было указано выше, на плате, имеющей несколько переключателей для согласования ее конфигурации с реальной аппаратной средой компьютера и может быть установлено в любое свободное гнездо расширения. Техническое обслуживание платы в процессе эксплуатации не требуется.

Для реализации предложенного способа устройство защиты от несанкционированного доступа к персональному компьютеру выполнено в виде платы с разъемами (на чертеже не показана), на которой расположены микроЭВМ типа Intel 8052, собственный ПЗУ BIOS и аппаратура подключения к персональному компьютеру и контактному устройству 36. Функциональное программное обеспечение предложенной

RU 2126168 C1

RU 2126168 C1

системы хранится в запоминающем устройстве и поэтому не может быть изменено в процессе работы Для связи с персональным компьютером используется одна из линий аппаратного прерывания Назначение этой линии жестко контролируется и не может быть изменено в процессе работы персонального компьютера.

Предложение может быть эффективно использовано на любом IBM совместимом компьютере с шиной ISA вне зависимости от типа операционной системы.

Формула изобретения:

1. Способ защиты персонального компьютера от несанкционированного доступа, заключающийся в том, что предварительно вводят идентификационные коды системы, предназначенные для хранения, вводят идентификационный код пользователя, сравнивают идентификационный код пользователя с идентификационными кодами системы, при совпадении указанного кода по крайней мере с одним из идентификационных кодов системы реализуют доступ к системе, отличающийся тем, что доступ к системе осуществляют путем замыкания цепи, соединяющей устройство ввода персонального компьютера с персональным компьютером.

2. Способ по п.1, отличающийся тем, что при реализации доступа к системе при совпадении указанных кодов формируют команду управления включением цепи, по которой осуществляют ее замыкание.

3. Устройство защиты персонального компьютера от несанкционированного доступа, содержащее микроЭВМ, запоминающее устройство, блок ввода идентификационного кода пользователя, схему сопряжения с персональным компьютером, отличающееся тем, что в устройство введены идентификатор кодов системы, формирователь блокировки, первый и второй входы-выходы микроЭВМ соединены с входами-выходами соответственно идентификатора кодов системы и блока ввода идентификационного кода пользователя, третий вход-выход соединен с управляющим входом формирователя сигнала блокировки, включенного в цепь устройства ввода персонального компьютера, соединенную с соответствующим входом схемы сопряжения с персональным компьютером, шина данных микроЭВМ соединена с шиной данных запоминающего устройства, управляющие выходы микроЭВМ соединены с первым и вторым управляющими входами запоминающего устройства, шина схемы сопряжения с персональным компьютером соединена с соответствующими шинами запоминающего устройства, управляющие выходы подключены к соответствующим входам запоминающего устройства.

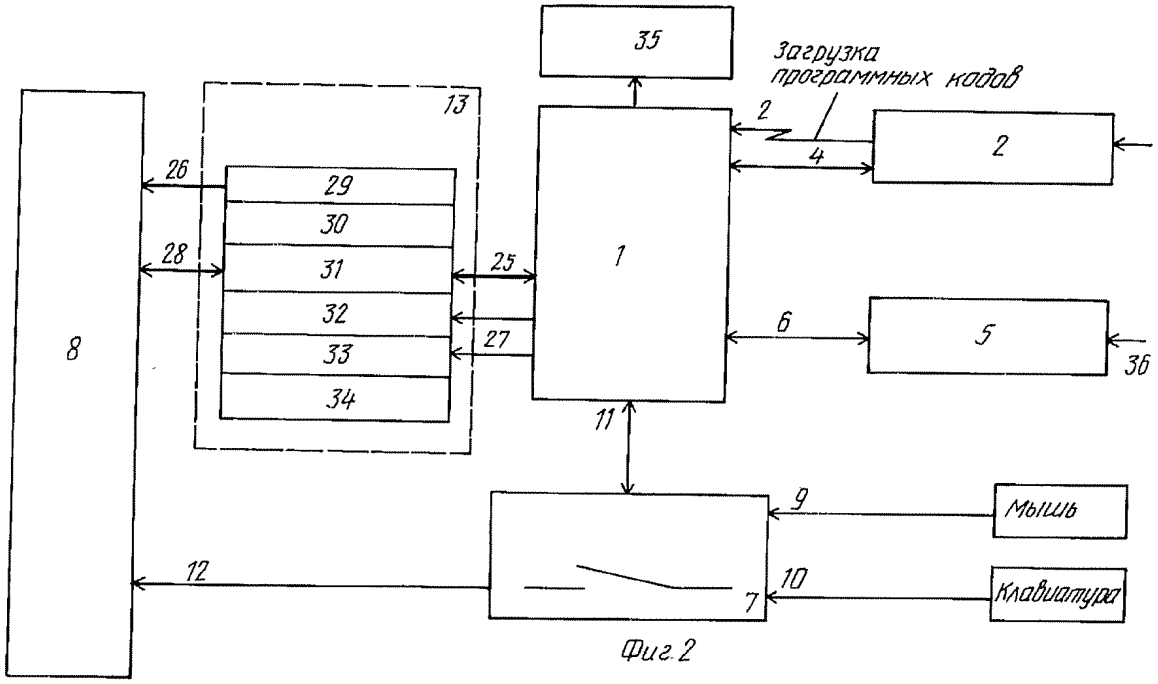
4. Устройство по п.3, отличающееся тем, что в него введен звукоизлучатель, соединенный с сигнальным выходом микроЭВМ.

5. Устройство по п.3, отличающееся тем, что формирователь сигнала блокировки выполнен в виде управляемого размыкающего ключа.

6. Устройство по п.3, отличающееся тем, что идентификатор кодов системы выполнен в виде энергонезависимого блока памяти.

RU 2126168 C1

RU 2126168 C1



Фиг. 2

RU 2126168 C1

RU 2126168 C1